UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

DAWN ARCHAMBEAU and **SHANTA MALONE,** on behalf of themselves and all others similarly situated, Plaintiffs, v. **GARDAWORLD CORPORATION d/b/a GARDAWORLD CASH** and **GARDAWORLD CASH SERVICES, INC. d/b/a GARDAWORLD CASH** Defendants.	Case No. JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Dawn Archambeau and Shanta Malone ("Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against GardaWorld Corporation d/b/a GardaWorld Cash and GardaWorld Cash Services, Inc. d/b/a/ GardaWorld Cash. ("GardaWorld" or "Defendants") based upon personal knowledge with respect to themselves and on information and belief derived from, among other things, investigation by their counsel and review of public documents as to all other matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against GardaWorld for its failure to properly secure and safeguard Plaintiffs' and other similarly situated GardaWorld employees' personally identifiable information ("PII") and protected health information ("PHI"), including names, Social Security numbers, Driver's License numbers, date(s) of birth, and/or insurance, benefit, or other health-related information (the "Private Information"), from criminal hackers.

2. GardaWorld is a private security and asset protection company that serves thousands of clients worldwide.

3. On or about March 22, 2024, GardaWorld filed official notice of a hacking incident with the Maine Office of the Attorney General.[1] Under state and federal law, organizations must report breaches involving PHI within at least sixty (60) days.

4. On or around the same time, GardaWorld also sent out data breach letters (the "Notice") to individuals whose information was compromised as a result of the hacking incident.

5. Based on the Notice sent to Plaintiffs and "Class Members" (defined below), unusual activity was detected on some of their computer systems and, in response, Defendants launched an investigation that revealed that an unauthorized party had access to certain administrative files that contained sensitive employee information. The investigation further determined that such access took place between October 30, 2023 and November 16, 2023 (the "Data Breach"). Yet, GardaWorld waited four months to notify the public that they were at risk.

6. As a result of this delayed response, Plaintiffs and Class Members had no idea for more than four months that their Private Information had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

7. The Private Information compromised in the Data Breach contained highly sensitive employee data, representing a gold mine for data thieves. The data included, but is not limited to, Social Security numbers, Driver's License numbers, date(s) of birth, and/or insurance, benefit, or other health-related information that GardaWorld collected and maintained.

[1] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/b259cad1-d4ba-46cf-9a2a-05ff391ebfcc.shtml (last visited Apr. 2, 2024).

8. Armed with the Private Information accessed in the Data Breach (and a head start), data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

9. There has been no assurance offered by Defendants that all personal data or copies of data have been recovered or destroyed, or that Defendants have adequately enhanced their data security practices sufficient to avoid a similar breach of their network in the future.

10. Therefore, Plaintiffs and Class Members have suffered and are at an imminent, immediate, and continuing increased risk of suffering, ascertainable losses in the form of harm from identity theft and other fraudulent misuse of their Private Information, the loss of the benefit of their bargain, out-of-pocket expenses incurred to remedy or mitigate the effects of the Data Breach, and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

11. Plaintiffs bring this class action lawsuit to address GardaWorld's inadequate safeguarding of their and Class Members' Private Information that it collected and maintained, and its failure to provide timely and adequate notice to Plaintiffs and Class Members of the types of information that were accessed, and that such information was subject to unauthorized access by cybercriminals.

12. The potential for improper disclosure and theft of Plaintiffs' and Class Members' Private Information was a known risk to GardaWorld, and thus GardaWorld was on notice that failing to take necessary steps to secure the Private Information left it vulnerable to an attack.

13. Upon information and belief, GardaWorld failed to properly monitor and implement adequate data security practices with regard to the computer network and systems that housed the Private Information. Had GardaWorld properly monitored its networks, it would have discovered the Breach sooner.

14. Plaintiffs' and Class Members' identities are now at risk because of GardaWorld's negligent conduct as the Private Information that GardaWorld collected and maintained is now in the hands of data thieves and other unauthorized third parties.

15. Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed and/or compromised during the Data Breach.

16. Accordingly, Plaintiffs, on behalf of themselves and the Class, assert claims for negligence, negligence *per se*, breach of implied contract, unjust enrichment, and declaratory judgment.

II. PARTIES

17. Plaintiff Dawn Archambeau is, and at all times mentioned herein was, an individual citizen of the State of Michigan.

18. Plaintiff Shanta Malone is, and at all times mentioned herein was, an individual citizen of the State of Michigan.

19. Defendant GardaWorld Corporation d/b/a GardaWorld Cash is a Canadian-based private security firm that conducts substantial business in the United States, including but not limited to, providing its cash management and other related services in Florida .

20. Defendant GardaWorld Cash Services, Inc. d/b/a GardaWorld Cash is incorporated in Delaware with its principal place of business at 2000 NW Corporate Blvd, Boca Raton, Florida 33424.[2]

III. JURISDICTION AND VENUE

21. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is over 100, many of whom have different citizenship from GardaWorld. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

22. This Court has jurisdiction over GardaWorld because GardaWorld operates in this District, which operations include the maintenance of the administrative files impacted in the Data Breach.

23. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District and GardaWorld has harmed Class Members residing in this District.

IV. FACTUAL ALLEGATIONS

A. GardaWorld's Business and Collection of Plaintiffs' and Class Members' Private Information

[2] *See* https://apps.web.maine.gov/online/aeviewer/ME/40/b259cad1-d4ba-46cf-9a2a-05ff391ebfcc.shtml (last visited Apr. 3, 2024).

24. GardaWorld Corporation is a private security firm that offers asset protection and cash management services to its clients. Founded in 1995, GardaWorld has 425 branch offices across 45 countries. GardaWorld Cash specifically focuses on providing cash-management solutions to its clients, which solutions include, without limitation, Cash Vault services, ATM management, secure transit, and cash automation. Upon information and belief, GardaWorld employs more than 132,000 people and generates approximately $3.9 billion in annual revenue.[3]

25. As a condition of employment, GardaWorld requires that its employees entrust it with highly sensitive personal and health information. In the ordinary course of employment, Plaintiffs and Class Members were required to provide their Private Information to Defendants.

26. In its Privacy Policy, GardaWorld states "we understand the importance of respecting privacy and are committed to protecting your personal data."[4] GardaWorld also states "we have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know."[5]

27. Thus, due to the highly sensitive and personal nature of the information GardaWorld acquires and stores with respect to its employees, GardaWorld, upon information and belief, promises to, among other things: keep employees' Private Information private; comply with industry standards related to data security and the maintenance of its employees' Private Information; inform its employees of its legal duties relating to data security and comply with all federal and state laws protecting employees' Private Information; only use and release employees'

[3] *See* https://www.jdsupra.com/legalnews/gardaworld-cash-notifies-consumers-of-8951681/ (last visited Apr. 2, 2024).
[4] *See* https://cash.garda.com/privacy-policy (last visited Apr. 2, 2024).
[5] *Id.*

Private Information for reasons that relate to the services it provides; and provide adequate notice to employees if their Private Information is disclosed without authorization.

28. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, GardaWorld assumed legal and equitable duties owed to them and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure and exfiltration.

29. Plaintiffs and Class Members relied on GardaWorld to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendants ultimately failed to do.

B. The Data Breach and Defendants' Inadequate Notice to Plaintiffs and Class Members

30. According to Defendants' Notice, they learned of unauthorized access to their computer systems on November 16, 2023, with such unauthorized access having taken place between October 30, 2023 and November 16, 2023.

31. Through the Data Breach, the unauthorized cybercriminal(s) accessed a cache of highly sensitive Private Information, including names, Social Security numbers, Driver's License numbers, date(s) of birth, and/or insurance, benefit, or other health-related information.

32. On or about March 22, 2024, roughly four months after GardaWorld learned that the Class's Private Information was first accessed by cybercriminals, GardaWorld finally began to notify its employees that the investigation determined that their Private Information was impacted.

33. GardaWorld had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class Members to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

34. Plaintiffs and Class Members provided their Private Information to GardaWorld with the reasonable expectation and mutual understanding that GardaWorld would comply with its obligations to keep such Information confidential and secure from unauthorized access and to provide timely notice of any security breaches.

35. GardaWorld's data security obligations were particularly important given the substantial increase in cyberattacks in recent years.

36. GardaWorld knew or should have known that its electronic records would be targeted by cybercriminals.

37. As an employer, GardaWorld knew, or should have known, the importance of safeguarding its employees' Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be imposed on GardaWorld's employees as a result of a breach. GardaWorld failed, however, to take adequate cybersecurity measures to prevent the Data Breach from occurring.

C. GardaWorld Failed to Comply with HIPAA

38. Title II of HIPAA contains what are known as the Administration Simplification provisions. *See* 42 U.S.C. §§ 1301, *et seq*. These provisions require that the Department of Health and Human Services ("HHS") create rules to streamline the standards for handling PHI similar to the data Defendants left unguarded and vulnerable to attack. The HHS has subsequently promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

39. GardaWorld's Data Breach resulted from a combination of insufficiencies that indicate GardaWorld failed to comply with safeguards mandated by HIPAA regulations and industry standards. First, it can be inferred from GardaWorld's Data Breach that GardaWorld

either failed to implement, or inadequately implemented, information security policies or procedures to protect Plaintiffs' and Class Members' PHI.

40. Plaintiffs' and Class Members' Private Information compromised in the Data Breach included "protected health information" as defined by CFR § 160.103.

41. 45 CFR § 164.402 defines "breach" as "the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information."

42. 45 CFR § 164.402 defines "unsecured protected health information" as "protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the [HHS] Secretary[.]"

43. Plaintiffs' and Class Members' Private Information included "unsecured protected health information" as defined by 45 CFR § 164.402.

44. Plaintiffs' and Class Members' unsecured PHI was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

45. Based upon Defendants' Notice to Plaintiffs and Class Members, GardaWorld reasonably believes that Plaintiffs' and Class Members' unsecured PHI has been acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

46. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

47. GardaWorld reasonably believes that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR,

Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

48. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

49. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

50. GardaWorld reasonably believes that Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

51. It is reasonable to infer that Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

52. It should be rebuttably presumed that unsecured PHI acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized persons.

53. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future

harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

54. In addition, GardaWorld's Data Breach could have been prevented if GardaWorld had implemented HIPAA mandated, industry standard policies and procedures for securely disposing of PHI when it was no longer necessary and/or had honored its obligations to its employees.

55. GardaWorld's security failures also include, but are not limited to:

a. Failing to maintain an adequate data security system to prevent data loss;

b. Failing to mitigate the risks of a data breach and loss of data;

c. Failing to ensure the confidentiality and integrity of electronic protected health information GardaWorld creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);

d. Failing to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights in violation of 45 CFR 164.312(a)(1);

e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);

f. Failing to identify and respond to suspected or known security incidents;

g. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);

h. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);

i. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3);

j. Failing to ensure compliance with HIPAA security standard rules by Defendants' workforce, in violation of 45 CFR 164.306(a)(94); and

k. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

56. The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 also required GardaWorld to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***" (emphasis added).

57. Because GardaWorld has failed to comply with HIPAA, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is also necessary to ensure GardaWorld's approach to information security is adequate and appropriate going forward. GardaWorld still maintains the PHI and other highly sensitive PII of their current and former employees, including Plaintiffs and Class Members. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of subsequent data breaches.

D. GardaWorld Failed to Comply with FTC Guidelines

58. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

59. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

60. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

61. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

62. As evidenced by the Data Breach, GardaWorld failed to properly implement basic data security practices. GardaWorld's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiffs' and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

63. GardaWorld was at all times fully aware of its obligation to protect the Private Information of its employees yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so.

E. GardaWorld Failed to Comply with Industry Standards

64. As noted above, experts studying cybersecurity routinely identify businesses as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

65. Some industry best practices that should be implemented by businesses dealing with sensitive PHI like GardaWorld include but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, and limiting which employees can access sensitive data. As evidenced by the Data Breach, Defendants failed to follow some or all of these industry best practices.

66. Other best cybersecurity practices that are standard in the industry include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points. As evidenced by the Data Breach, Defendants failed to follow these cybersecurity best practices.

67. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

68. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

F. GardaWorld Breached its Duty to Safeguard Plaintiffs' and Class Members' Private Information

69. In addition to its obligations under federal and state laws, GardaWorld owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. GardaWorld owed a duty to Plaintiffs and Class Members to provide reasonable security, including consistency with industry standards and requirements, and to ensure that its computer systems, networks, and protocols adequately protected the Private Information of Class Members

70. GardaWorld breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. GardaWorld's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system that would reduce the risk of data breaches and cyberattacks;

b. Failing to adequately protect employees' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to sufficiently train its employees regarding the proper handling of employees' Private Information;

e. Failing to fully comply with FTC guidelines for cybersecurity in violation of the FTCA;

f. Failing to adhere to HIPAA and industry standards for cybersecurity as discussed above; and

g. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class Members' Private Information.

71. GardaWorld negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access its computer network and systems which contained unsecured and unencrypted Private Information.

72. Had GardaWorld remedied the deficiencies in its information storage and security systems, followed industry guidelines, and adopted security measures recommended by experts in the field, they could have prevented intrusion into its information storage and security systems and, ultimately, the theft of Plaintiffs' and Class Members' confidential Private Information.

73. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's more, they have been harmed as a result of the Data Breach and now face an increased risk of future harm that includes, but is not limited to, fraud and identity theft. Plaintiffs and Class Members also lost the benefit of the bargain they made with GardaWorld.

G. GardaWorld Should Have Known that Cybercriminals Target PII and PHI to Carry Out Fraud and Identity Theft

74. The FTC hosted a workshop to discuss "informational injuries," which are injuries that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such as data breaches or unauthorized disclosure of data.[6] Exposure of highly sensitive personal information that a consumer wishes to keep private may cause harm to the consumer, such as the ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them of the benefits provided by the full range of goods and services available which can have negative impacts on daily life.

75. Any victim of a data breach is exposed to serious ramifications regardless of the nature of the data that was breached. Indeed, the reason why criminals steal information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims or to take over victims' identities in order to engage in illegal financial transactions under the victims' names.

76. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or to otherwise harass or track the victim. For example, armed with just a name and date of birth, a

[6] *FTC Information Injury Workshop, BE and BCP Staff Perspective,* Federal Trade Commission, (October 2018), *available at* https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf (last visited on Apr. 2, 2024).

data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

77. In fact, as technology advances, computer programs may scan the Internet with a wider scope to create a mosaic of information that may be used to link compromised information to an individual in ways that were not previously possible. This is known as the "mosaic effect." Names and dates of birth, combined with contact information like telephone numbers and email addresses, are very valuable to hackers and identity thieves as it allows them to access users' other accounts.

78. Thus, even if certain information were not purportedly involved in the Data Breach, the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide variety of fraudulent activity against Plaintiffs and Class Members.

79. One such example of this is the development of "Fullz" packages.

80. Cybercriminals can cross-reference two sources of the Private Information compromised in the Data Breach to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

81. The development of "Fullz" packages means that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and the proposed Class's phone numbers, email addresses, and other sources and identifiers. In other words, even if

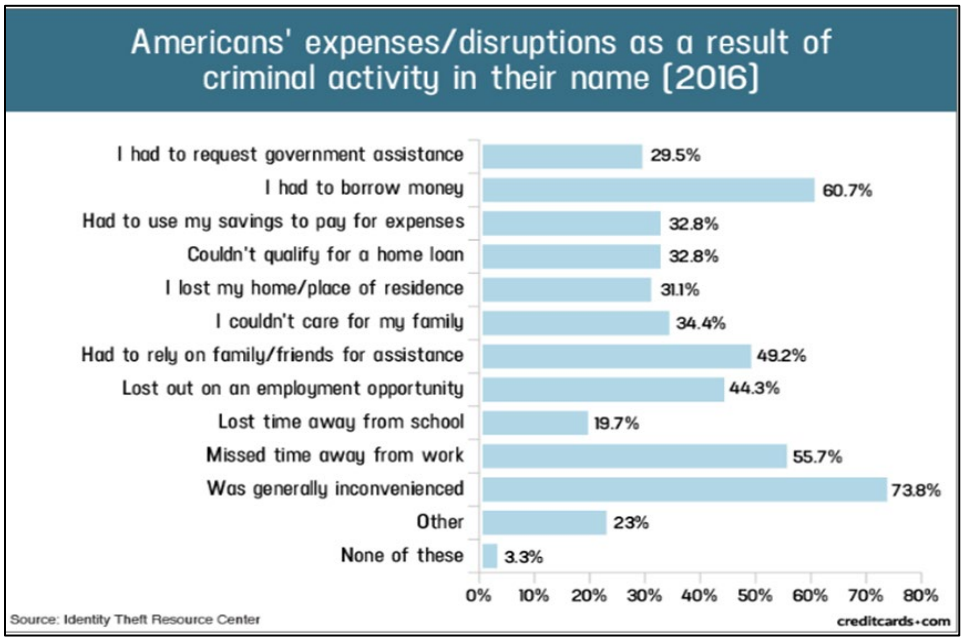
certain information such as emails, phone numbers, or credit card or financial account numbers may not be included in the Private Information stolen in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

82. For these reasons, the FTC recommends that identity theft victims take several time-consuming steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert on their account (and an extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a freeze on their credit, and correcting their credit reports.[7] However, these steps do not guarantee protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

83. Identity thieves can also use stolen personal information such as Social Security numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank fraud, to obtain a driver's license or official identification card in the victim's name but with the thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house in the victim's name, receive medical services in the victim's name, and even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

[7] *See IdentityTheft.gov,* Federal Trade Commission, *available at* https://www.identitytheft.gov/Steps (last visited Apr. 2, 2024).

84. In fact, a study by the Identity Theft Resource Center[8] shows the multitude of harms caused by fraudulent use of PII:



85. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.[9]

86. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

87. While credit card information and associated PII can sell for as little as $1-$2 on the black market, protected health information can sell for as much as $363 according to the Infosec Institute.[10]

---

[8] Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), *available at* https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/ (last visited on Apr. 2, 2024).

[9] Federal Trade Commission, *Warning Signs of Identity Theft, available at*: https://consumer.ftc.gov/articles/what-know-about-identity-theft (last visited on Apr. 2, 2024).

[10] Center for Internet Security, *Data Breaches: In the Healthcare Sector, available at*: https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector (last visited on Apr. 2, 2024).

88. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

89. Medical identity theft can result in inaccuracies in medical records and costly false claims. It can also have life-threatening consequences. If a victim's health information is mixed with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[11]

90. The ramifications of GardaWorld's failure to keep its employees' Private Information secure are long-lasting and severe. Once it is stolen, fraudulent use of such and damage to victims may continue for years.

91. Here, not only was sensitive medical information compromised, but Social Security numbers were compromised too. The value of both PII and PHI is axiomatic. The value of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

92. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and also between when PII and/or PHI is stolen and when it is

[11] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, *available at*: https://kffhealthnews.org/news/rise-of-indentity-theft/ (last visited on Apr. 2, 2024).

misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:[12]

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

93. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

94. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

H. Plaintiffs' and Class Members' Damages

Plaintiff Dawn Archambeau's Experience

95. When Plaintiff Archambeau became an employee, Defendants required Plaintiff Archambeau provide them with substantial amounts of her Private Information, including PHI.

96. On or about March 22, 2024, Plaintiff Archambeau received a letter entitled "Notice of Data Breach" which told her that her Private Information had been accessed during the Data Breach. The notice letter informed her that the Private Information accessed included her "name, Social Security number, Driver's License, date of birth, and/or insurance, benefit, or other health-related information."

[12] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), *available at* https://www.gao.gov/assets/270/262904.html (last visited Apr. 2, 2024).

97. The notice letter offered Plaintiff Archambeau only two years of credit monitoring services. Two years of credit monitoring is not sufficient given that Plaintiff Archambeau will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

98. Plaintiff Archambeau suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

99. Plaintiff Archambeau would not have provided her Private Information to Defendants had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard their employees' personal and health information from theft, and that those systems were subject to a data breach.

100. Plaintiff Archambeau suffered actual injury in the form of having her PII and PHI compromised and/or stolen as a result of the Data Breach.

101. Plaintiff Archambeau suffered actual injury in the form of damages to and diminution in the value of her personal and health information – a form of intangible property that Plaintiff Archambeau entrusted to Defendants for employment purposes, and which was compromised in, and as a result of, the Data Breach.

102. Plaintiff Archambeau suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

103. Plaintiff Archambeau has a continuing interest in ensuring that her PII and PHI, which remain in the possession of Defendants, are protected and safeguarded from future breaches.

104. As a result of the Data Breach, Plaintiff Archambeau made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendants. Plaintiff Archambeau has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

105. As a result of the Data Breach, Plaintiff Archambeau has suffered anxiety as a result of the release of her PII and PHI, which she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of committing cyber and other crimes against her including, but not limited to, fraud and identity theft. Plaintiff Archambeau is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on her life.

106. Plaintiff Archambeau also suffered actual injury from having her Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of her PII and PHI, a form of property that Defendants obtained from Plaintiff Archambeau; (b) violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

107. As a result of the Data Breach, Plaintiff Archambeau anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

Plaintiff Shanta Malone's Experience

108. When Plaintiff Malone became an employee, Defendants required Plaintiff Archambeau to provide them with substantial amounts of her Private Information, including PHI.

109. On or about March 22, 2024, Plaintiff Malone received a letter entitled "Notice of Data Breach" which told her that her Private Information had been accessed during the Data Breach. The notice letter informed her that the Private Information impacted included her "name, Social Security number, Driver's License number, date of birth, and/ or insurance, benefit, or other health-related information."

110. The notice letter offered Plaintiff Malone only two years of credit monitoring services. Two years of credit monitoring is not sufficient given that Plaintiff Malone will now experience a lifetime of increased risk of identity theft, including but not limited to, potential medical fraud.

111. Plaintiff Malone suffered actual injury in the form of time spent dealing with the Data Breach and the increased risk of fraud resulting from the Data Breach and/or monitoring her accounts for fraud.

112. Plaintiff Malone would not have provided her Private Information to Defendants had Defendants timely disclosed that their systems lacked adequate computer and data security practices to safeguard their employees' personal and health information from theft, and that those systems were subject to a data breach.

113. Plaintiff Malone suffered actual injury in the form of having her PII and PHI compromised and/or stolen as a result of the Data Breach.

114. Plaintiff Malone suffered actual injury in the form of damages to and diminution in the value of her personal and health information – a form of intangible property that Plaintiff

Malone entrusted to Defendants for employment purposes, which was compromised in, and as a result of the Data Breach.

115. Plaintiff Malone suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals.

116. Plaintiff Malone has a continuing interest in ensuring that her PII and PHI, which remain in the possession of Defendants, are protected and safeguarded from future breaches.

117. As a result of the Data Breach, Plaintiff Malone made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing financial accounts for any indications of actual or attempted identity theft or fraud, and researching the credit monitoring offered by Defendants. Plaintiff Malone has spent several hours dealing with the Data Breach, valuable time she otherwise would have spent on other activities.

118. As a result of the Data Breach, Plaintiff Malone has suffered anxiety as a result of the release of her PII and PHI, which she believed would be protected from unauthorized access and disclosure. These feelings include anxiety about unauthorized parties viewing, selling, and/or using her PII and PHI for purposes of committing cyber and other crimes against her including, but not limited to, fraud and identity theft. Plaintiff Archambeau is very concerned about this increased, substantial, and continuing risk, as well as the consequences that identity theft and fraud resulting from the Data Breach would have on her life.

119. Plaintiff Malone also suffered actual injury from having her Private Information compromised as a result of the Data Breach in the form of (a) damage to and diminution in the value of her PII and PHI, a form of property that Defendants obtained from Plaintiff Malone; (b)

violation of her privacy rights; and (c) present, imminent, and impending injury arising from the increased risk of identity theft, and fraud she now faces.

120. As a result of the Data Breach, Plaintiff Malone anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the many harms caused by the Data Breach.

121. In sum, Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach.

122. Plaintiffs and Class Members entrusted their Private Information to Defendants as a condition of employment.

123. Their Private Information was subsequently compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from Defendants' inadequate data security practices.

124. As a direct and proximate result of GardaWorld's actions and omissions, Plaintiffs and Class Members have been harmed and are at an imminent, immediate, and continuing increased risk of harm, including but not limited to, having medical services billed in their names, loans opened in their names, tax returns filed in their names, utility bills opened in their names, credit card accounts opened in their names, and other forms of identity theft.

125. Further, and as set forth above, as a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have also been forced to take the time and effort to mitigate the actual and potential impact of the data breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

126. Plaintiffs and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

127. Plaintiffs and Class Members also face a substantial risk of being targeted in future phishing, data intrusion, and other illegal schemes through the misuse of their Private Information, since potential fraudsters will likely use such Private Information to carry out such targeted schemes against Plaintiffs and Class Members.

128. The Private Information maintained by and stolen from Defendants' systems, combined with publicly available information, allows nefarious actors to assemble a detailed mosaic of Plaintiffs and Class Members, which can also be used to carry out targeted fraudulent schemes against Plaintiffs and Class Members.

129. Additionally, Plaintiffs and Class Members also suffered a loss of value of their PII and PHI when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[13] In fact, consumers who agree to provide their web browsing history to the Nielsen Corporation can in turn receive up to $50 a year.[14]

130. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and illegal markets, has been harmed and diminished due to its acquisition by cybercriminals. This transfer of valuable information

[13] *See* https://thequantumrecord.com/blog/data-brokers-profit-from-our-data/#:~:text=The%20business%20of%20data%20brokering,annual%20revenue%20of%20%24200%20billion. (last visited on Apr. 2, 2024).

[14] *Frequently Asked Questions,* Nielsen Computer & Mobile Panel, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited on Apr. 2, 2024).

happened with no consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is apparently readily available to others, and the rarity of the Private Information has been destroyed because it is no longer only held by Plaintiffs and the Class Members, and because that data no longer necessarily correlates only with activities undertaken by Plaintiffs and the Class Members, thereby causing additional loss of value.

131. Finally, Plaintiffs and Class Members have suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach.

132. Moreover, Plaintiffs and Class Members have an interest in ensuring that their Private Information, which is believed to still be in the possession of GardaWorld, is protected from future breaches by the implementation of more adequate data security measures and safeguards, including but not limited to, ensuring that the storage of data or documents containing highly sensitive personal and health information of its employees is not accessible online, that access to such data is password-protected, and that such data is properly encrypted.

133. As a direct and proximate result of GardaWorld's actions and inactions, Plaintiffs and Class Members have suffered a loss of privacy and have suffered cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

134. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

135. Specifically, Plaintiffs propose the following Nationwide Class definition (referred to herein as the "Class"), subject to amendment as appropriate:

Nationwide Class

> All individuals in the United States who had Private Information accessed and/ or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

136. Excluded from the Class are Defendants and their parents or subsidiaries, any entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

137. Plaintiffs reserve the right to modify or amend the definitions of the proposed Nationwide Class, as well as add subclasses before the Court determines whether certification is appropriate.

138. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

139. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact number and identities of Class Members are unknown at this time, based on information and belief, the Class consists of 39,928 current and former employees of GardaWorld whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through GardaWorld's records, Class Members' records, publication notice, self-identification, and other means.

140. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether GardaWorld engaged in the conduct alleged herein;

b. Whether GardaWorld's conduct violated the FTCA and HIPAA;

c. When GardaWorld learned of the Data Breach;

d. Whether GardaWorld's response to the Data Breach was adequate;

e. Whether GardaWorld unlawfully lost or disclosed Plaintiffs' and Class Members' Private Information;

f. Whether GardaWorld failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

g. Whether GardaWorld's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether GardaWorld's data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether GardaWorld owed a duty to Class Members to safeguard their Private Information;

j. Whether GardaWorld breached its duty to Class Members to safeguard their Private Information;

k. Whether hackers obtained Class Members' Private Information via the Data Breach;

l. Whether GardaWorld had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class Members;

m. Whether GardaWorld breached its duty to provide timely and accurate notice of the Data Breach to Plaintiffs and Class Members;

n. Whether GardaWorld knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiffs and Class Members suffered as a result of GardaWorld's misconduct;

p. Whether GardaWorld's conduct was negligent;

q. Whether GardaWorld's conduct was *per se* negligent;

r. Whether GardaWorld was unjustly enriched;

s. Whether Plaintiffs and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

t. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

141. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of GardaWorld. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

142. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

143. Predominance. GardaWorld has engaged in a common course of conduct toward Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common

issues arising from GardaWorld's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

144. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for GardaWorld. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

145. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). GardaWorld has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

146. Finally, all members of the proposed Class are readily ascertainable. GardaWorld has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by GardaWorld.

CLAIMS FOR RELIEF

COUNT I
NEGLIGENCE
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

147. Plaintiffs restate and reallege allegations stated from paragraphs 1-146 as if fully set forth herein.

148. GardaWorld knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

149. GardaWorld's duty also included a responsibility to implement processes by which they could detect and analyze a breach of its security systems quickly and to give prompt notice to those affected in the case of a cyberattack.

150. GardaWorld knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. GardaWorld was on notice because, on information and belief, they knew or should have known that they would be an attractive target for cyberattacks.

151. GardaWorld owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to them. GardaWorld's duties included, but were not limited to, the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in its possession;

b. To protect employees' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;

c. To have procedures in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to HIPAA and the FTCA;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

152. GardaWorld's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

153. GardaWorld's duty also arose because Defendants were bound by industry standards to protect its employees' confidential Private Information.

154. Plaintiffs and Class Members were foreseeable victims of any inadequate security practices on the part of Defendants, and GardaWorld owed them a duty of care to not subject them to an unreasonable risk of harm.

155. GardaWorld, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' Private Information within GardaWorld's possession.

156. GardaWorld, by its actions and/or omissions, breached its duty of care by failing to provide, or acting with reckless disregard for, fair, reasonable, or adequate computer systems and data security practices to safeguard the Private Information of Plaintiffs and Class Members.

157. GardaWorld, by its actions and/or omissions, breached its duty of care by failing to promptly identify the Data Breach and then failing to provide prompt notice of the Data Breach to the persons whose Private Information was compromised.

158. GardaWorld breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system maintained reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to comply with the FTCA;

f. Failing to detect in a timely manner that Class Members' Private Information had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

159. GardaWorld acted with reckless disregard for the rights of Plaintiffs and Class Members by failing to provide prompt and adequate individual notice of the Data Breach such that

Plaintiffs and Class Members could take measures to protect themselves from damages caused by the fraudulent use of the Private Information compromised in the Data Breach.

160. GardaWorld had a special relationship with Plaintiffs and Class Members. Plaintiffs' and Class Members' willingness to entrust GardaWorld with their Private Information was predicated on the understanding that GardaWorld would take adequate security precautions. Moreover, only GardaWorld had the ability to protect its systems (and the Private Information that it stored on them) from attack.

161. GardaWorld's breach of duties owed to Plaintiffs and Class Members caused Plaintiffs' and Class Members' Private Information to be compromised and exfiltrated as alleged herein.

162. As a result of GardaWorld's ongoing failure to notify Plaintiffs and Class Members regarding exactly what Private Information has been compromised, Plaintiffs and Class Members have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

163. GardaWorld's breaches of duty also caused a substantial, imminent risk to Plaintiffs and Class Members of identity theft, loss of control over their Private Information, and/or loss of time and money to monitor their accounts for fraud.

164. As a result of GardaWorld's negligence in breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private Information, which is still in the possession of third parties, will be used for fraudulent purposes.

165. GardaWorld also had independent duties under state laws that required them to reasonably safeguard Plaintiffs' and Class Members' Private Information and promptly notify them about the Data Breach.

166. As a direct and proximate result of GardaWorld's negligent conduct, Plaintiffs and Class Members have suffered damages as alleged herein and are at imminent risk of further harm.

167. The injury and harm that Plaintiffs and Class Members suffered was reasonably foreseeable.

168. Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

169. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring GardaWorld to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT II
NEGLIGENCE *PER SE*
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

170. Plaintiffs restate and reallege allegations stated from paragraphs 1-146 as if fully set forth herein.

171. Pursuant to Section 5 of the FTCA, GardaWorld had a duty to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiffs and Class Members.

172. Pursuant to HIPAA, 42 U.S.C. § 1302(d), *et seq*., GardaWorld had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Private Information.

173. Specifically, pursuant to HIPAA, Defendants had a duty to render the electronic PHI it maintained unusable, unreadable, or indecipherable to unauthorized individuals by "the use of an algorithmic process to transform data into a form in which there is a low probability of

assigning meaning without the use of a confidential process or key." *See* definition of "encryption" at 45 C.F.R. § 164.304.

174. GardaWorld breached its duties to Plaintiffs and Class Members under the FTCA and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

175. Specifically, GardaWorld breached its duties by failing to employ industry-standard cybersecurity measures in order to comply with the FTCA, including but not limited to proper segregation, access controls, password protection, encryption, intrusion detection, secure destruction of unnecessary data, and penetration testing.

176. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice of failing to use reasonable measures to protect PII and PHI (such as the Private Information compromised in the Data Breach). The FTC rulings and publications described above, together with the industry-standard cybersecurity measures set forth herein, form part of the basis of GardaWorld's duty in this regard.

177. GardaWorld also violated the FTCA and HIPAA by failing to use reasonable measures to protect the Private Information of Plaintiffs and the Class and by not complying with applicable industry standards, as described herein.

178. It was reasonably foreseeable, particularly given the growing number of data breaches of Private Information, that the failure to reasonably protect and secure Plaintiffs' and Class Members' Private Information in compliance with applicable laws would result in an unauthorized third-party gaining access to GardaWorld's networks, databases, and computers that stored Plaintiffs' and Class Members' unencrypted Private Information.

179. Plaintiffs and Class Members are within the class of persons that the FTCA and HIPAA are intended to protect and GardaWorld's failure to comply with both constitutes negligence *per se*.

180. Plaintiffs' and Class Members' Private Information constitutes personal property that was stolen due to GardaWorld's negligence, resulting in harm, injury, and damages to Plaintiffs and Class Members.

181. As a direct and proximate result of GardaWorld's negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the unauthorized access of their Private Information, including but not limited to damages from the lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives.

182. As a direct and proximate result of GardaWorld's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to compensatory and consequential damages in an amount to be proven at trial.

183. In addition to monetary relief, Plaintiffs and Class Members are also entitled to injunctive relief requiring GardaWorld to, *inter alia*, strengthen its data security systems and monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

COUNT III
BREACH OF IMPLIED CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

184. Plaintiffs restate and reallege allegations stated from paragraphs 1-146 as if fully set forth herein.

185. GardaWorld provided employment to Plaintiffs and Class Members.

186. Defendants, as an employer, held the Private Information on behalf of Plaintiffs and Class Members. Holding Plaintiffs and Class Members' Private Information was part of Defendants' regular business practices, as agreed by the parties. When Plaintiffs and Class Members joined Defendants' employment, they agreed to have their Private Information stored in Defendants' network.

187. Plaintiffs and Class Members entered implied contracts with Defendants in which Defendants agreed to safeguard and protect such Information and to timely detect any breaches of their Private Information. Plaintiffs and Class Members were required to share Private Information to obtain employment. In entering such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

188. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendants.

189. As consideration, Plaintiffs and Class Members turned over valuable Private Information to GardaWorld. Accordingly, Plaintiffs and Class Members bargained with GardaWorld to securely maintain and store their Private Information.

190. GardaWorld accepted possession of Plaintiffs' and Class Members' Private Information for employment purposes.

191. In providing their valuable Private Information to Defendants in exchange for Defendants' services, Plaintiffs and Class Members intended and understood that GardaWorld would adequately safeguard the Private Information as part of those services.

192. Defendants' implied promises to Plaintiffs and Class Members include, but are not limited to, (1) taking steps to ensure that anyone who is granted access to Private Information also

protect the confidentiality of that data; (2) taking steps to ensure that the Private Information that is placed in the control of their employees is restricted and limited to achieve an authorized business purpose; (3) restricting access to qualified and trained employees and/or agents; (4) designing and implementing appropriate retention policies to protect the Private Information against criminal data breaches; (5) applying or requiring proper encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA standards to make sure that Plaintiffs' and Class Members' PHI would remain protected; and (8) taking other steps to protect against foreseeable data breaches.

193. Defendants breached these implied promises they made with Plaintiff and Class Members by failing to safeguard and protect their Private Information and by failing to notify Plaintiff and Class Members thereof within a reasonable time.

194. Plaintiffs and Class Members would not have entrusted their Private Information to GardaWorld in the absence of such an implied contract.

195. Had GardaWorld disclosed to Plaintiffs and the Class that they did not have adequate computer systems and security practices to secure sensitive data, Plaintiffs and Class Members would not have provided their Private Information to GardaWorld.

196. As an employer, GardaWorld recognized (or should have recognized) that Plaintiffs' and Class Member's Private Information is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain with Plaintiffs and the other Class Members.

197. GardaWorld violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiffs' and Class Members' Private Information.

GardaWorld further breached these implied contracts by failing to comply with its promise to abide by HIPAA.

198. Additionally, GardaWorld breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic protected health information they created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

199. GardaWorld also breached the implied contracts with Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

200. GardaWorld further breached the implied contracts with Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

201. GardaWorld further breached the implied contracts with Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

202. GardaWorld further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

203. GardaWorld further breached the implied contracts with Plaintiffs and Class Members by failing to protect against any reasonably anticipated uses or disclosures of electronic

protected health information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

204. GardaWorld further breached the implied contracts with Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce violations, in violation of 45 CFR 164.306(a)(94).

205. GardaWorld further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq*.

206. GardaWorld further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

207. GardaWorld further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' PHI.

208. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide and accurate and complete Private Information to GardaWorld in exchange for GardaWorld's agreement to, *inter alia*, provide employment that included protection of their highly sensitive Private Information.

209. Plaintiffs and Class Members have been damaged by GardaWorld's conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT IV
UNJUST ENRICHMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

210. Plaintiffs restate and reallege allegations stated from paragraphs 1-146 as if fully set forth herein.

211. This Count is pleaded in the alternative to Count III above.

212. Plaintiffs and Class Members conferred a benefit on Defendants. Specifically, they provided Defendants with their Private Information, which Private Information has inherent value. In exchange, Plaintiffs and Class Members should have been entitled to have Defendants protect their Private Information with adequate data security, especially in light of their employer-employee relationship.

213. Defendants knew that Plaintiffs and Class Members conferred a benefit upon them and have accepted and retained that benefit by accepting and retaining the Private Information entrusted to them. Defendants profited from Plaintiffs' retained data and used Plaintiffs and Class Members' Private Information for business purposes.

214. Defendants failed to secure Plaintiffs' and Class Members' Private Information and, therefore, did not fully compensate Plaintiffs or Class Members for the value that their Private Information provided.

215. Defendants acquired the Private Information through inequitable record retention as they failed to disclose the inadequate security practices previously alleged.

216. If Plaintiffs and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to secure their Private Information, they would have made alternative employment choices that excluded Defendants.

217. Plaintiffs and Class Members have no adequate remedy at law.

218. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiffs and Class Members conferred upon it.

219. As a direct and proximate result of GardaWorld's conduct, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) the imminent and substantial risk of actual identity theft; (ii) the loss of the opportunity to control how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remains in GardaWorld's possession and is subject to further unauthorized disclosures so long as GardaWorld fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

220. Plaintiffs and Class Members are entitled to full refunds, restitution, and/or damages from GardaWorld and/or an order proportionally disgorging all profits, benefits, and other compensation obtained by GardaWorld from its wrongful conduct. This can be accomplished by establishing a constructive trust from which the Plaintiffs and Class Members may seek restitution or compensation.

221. Plaintiffs and Class Members may not have an adequate remedy at law against GardaWorld, and accordingly, they plead this claim for unjust enrichment in addition to, or in the alternative to, other claims pleaded herein.

COUNT V
DECLARATORY JUDGMENT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS)

222. Plaintiffs restate and reallege allegations stated from paragraphs 1-146 as if fully set forth herein.

223. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal laws and regulations described in this Complaint.

224. GardaWorld owes a duty of care to Plaintiffs and Class Members, which required them to adequately secure Plaintiffs' and Class Members' Private Information.

225. GardaWorld still possesses Private Information regarding Plaintiffs and Class Members.

226. Plaintiffs allege that GardaWorld's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

227. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. GardaWorld owes a legal duty to secure its employees' Private Information and to timely notify employees of a data breach under the common law, HIPAA, and the FTCA;

b. GardaWorld's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices that are appropriate to protect employees' Private Information; and

c. GardaWorld continues to breach this legal duty by failing to employ reasonable measures to secure employees' Private Information.

228. This Court should also issue corresponding prospective injunctive relief requiring GardaWorld to employ adequate security protocols consistent with legal and industry standards to protect employees' Private Information, including the following:

a. Order GardaWorld to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendants' explicit or implicit contractual obligations and duties of care, GardaWorld must implement and maintain reasonable security measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on GardaWorld's systems on a periodic basis, and ordering GardaWorld to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of GardaWorld's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its employees about the threats they face with regard to the security of their Private Information, as well as the steps they should take to protect themselves.

229. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at GardaWorld. The risk of another such breach is real, immediate, and substantial. If another breach at GardaWorld occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

230. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to GardaWorld if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of GardaWorld's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and GardaWorld has a pre-existing legal obligation to employ such measures.

231. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at

GardaWorld, thus preventing future injury to Plaintiffs and other employees whose Private Information would be further compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class described above, seek the following relief:

a. An order certifying this action as a Class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class requested herein;

b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order instructing GardaWorld to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;

e. An order requiring GardaWorld to pay the costs involved in notifying Class Members about the judgment and administering the claims process;

f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

g. An award of such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: April 3, 2024

Respectfully submitted,

/s/ Jessica Wallace

Jessica Wallace, Bar No. 1008325
Mason A. Barney (*pro hac vice* to be filed)
Tyler J. Bean (*pro hac vice* to be filed)
SIRI & GLIMSTAD LLP
20200 West Dixie Highway, Suite 902
Aventura, FL 33180
Tel: (786) 244-5660
E: jwallace@sirillp.com
E: mbarney@sirillp.com
E: tbean@sirillp.com